回帰符号系におけるBalanced Incomplete Block Designの応用について (情報理論・実験計画法における組合せ数学の諸問題研究会報告集)

AUTHOR(S):

岩垂, 好裕

CITATION:

岩垂, 好裕. 回帰符号系におけるBalanced Incomplete Block Designの応用について (情報理論・実験計画法における組合せ数学の諸問題研究会報告集). 数理解析研究所講究録 1970, 82: 41-51

ISSUE DATE:

1970-03

URL:

http://hdl.handle.net/2433/108042

数理解析研究所講究録
82巻 1970年 41-51

回帰符号系に於けるBalanced Incomplete Block Designの応用について

日本電気株式会社　岩垂好裕

1. 序

閾値復号が可能なブロック符号系の構成にBalanced Incomplete Block Designが用いられる事は、Rudolph [1], Weldon [2], Goethals et al [3], Weldon等により示されている。回帰符号系に於ても閾値復号法が一部用いられているが、現段階に於ては、少くも組織符号に限定する限りでは、パリティチェックマトリクス構成上の制限がブロック符号よりも大きい為、その応用の範囲は、Perfect Difference Setによって自己直交符号を導く、Robinson & Bernsteinの手法に限られている。[5]

本稿に於ては先ずRobinson & Bernsteinの自己直交符号を構成する手法を簡単に紹介し、次に同じくPerfect Difference Setから構成されるWeldonの符号[2]等のブロック符号と比較して回帰符号構成上の問題点を挙げ、更

に数学的に未解決のいくつかの回帰符号構成法を列挙する事とする。

2. Robinson & Bernstein の自己直交符号(5)

回帰符号は又畳みこみ符号ともいわれ、その符号構成はブロック符号の場合と同じくパリティチェックマトリクス H によって定められる。Massey の記法(6)に従えば 伝送速度 $R = 1/b$ 又は $b-1/b$ の符号は、$b-1$ 個のパリティ三角

$$H_1 = \begin{pmatrix} g_0^{(1)} & & & \\ g_1^{(1)} & g_0^{(1)} & & 0 \\ \vdots & & \ddots & \\ g_{m_1-1}^{(1)} & g_{m_1-2}^{(1)} & & g_0^{(1)} \end{pmatrix} \quad I_{m_1} \qquad (1)$$

$$\vdots$$

$$H_b = \begin{pmatrix} g_0^{(b)} & & & \\ g_1^{(b)} & g_0^{(b)} & & 0 \\ \vdots & & \ddots & \\ g_{m_b-1}^{(b)} & g_{m_b-2}^{(b)} & & g_0^{(b)} \end{pmatrix} \quad I_{m_b}$$

によって定められる。伝送符号を半無限列ベクトル $X_1, \cdots, X_b$ で表す時、$H_1 X_1 = 0, \cdots H_b X_b = 0$ の関係を満し、従って伝送路上の誤りを表す列ベクトル E_i, $i = 2, 3, \cdots, b$ に対して

$$H_i(X_i + E_i) = H_i E_i = S_i \qquad (2)$$

$$i = 2, 3, \cdots, b$$

がシンドローム系列 S_i, $i = 2, 3, \cdots, b$ を与える。

雑音ビット $e_0^{(i)}$, $i = 1, 2, \cdots b-1$ について直交する畳みこみ自己直交符号とは、どの２つのパリティチェックの式も、$e_0^{(i)}$ 以外の同じ二つの雑音ビットを含まない畳みこみ符号の事である。

例Ⅰ.（Hagelbarger）〔7〕,

$$H_2 = \begin{matrix} 1 & & & & & & & & \\ 0 & 1 & & & & & & & \\ 1 & 0 & 1 & & & O & & & \\ 0 & 1 & 0 & 1 & & & & & \\ 0 & 0 & 1 & 0 & 1 & & & & \\ 1 & 0 & 0 & 1 & 0 & 1 & & & \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & & \end{matrix} \quad I_7 \qquad (3)$$

は $R = 1/2$ の自己直交符号である。

(1)式及び(3)式で示されているように、自己直交符号の構成は、パリティ三角の Design に帰結される。これはブロック符号の構成が正方マトリクスの Design に帰結されるのに対して、回帰符号構成法の一つの特徴である。Robinson & Bernstein は Perfect Difference Set によってパリティ三角を構成する方法を与えた。

Perfect Difference Set は次の性質を持つ $q+1$ 個の整数の組 $(d_1, d_2, \cdots, d_{q+1})$ である。即ちその q^2+q 個の差

$d_i - d_j$, $i \neq j$, $i, j = 1, 2, \cdots, q+1$ が modulo q^2+q+1 で整数 $1, 2, \cdots, q^2+q$ に合同である。

例2. $(2, 4, 8)$ は mod 7 を持つ Perfect Difference Set である。即ち, $2-8 \equiv 1$, $4-2 \equiv 2$, $4-8 \equiv 3$, $8-4 \equiv 4$, $2-4 \equiv 5$, $8-2 \equiv 6$ $(\mathrm{mod}\ 7)$

一つの Difference Set が与えられた時. これから Regular Array を構成する. 即ち Regular Array の第1行 $(a_{11}, a_{12}, \cdots, a_{1,q+1})$ は Difference Set の継続する元の差

$$a_{1i} = d_{i+1} - d_i, \quad i = 1, 2, \cdots, q$$

$$a_{1,q+1} = q^2+q+1 + d_1 - d_{q+1}$$

残りの元は

$$a_{i,j} = \sum_{k=j}^{i+j-1} a_{1,k}$$

で与えられ. ここで $k > q+1$ に対しては $a_{1,k} = a_{1,k-q-1}$, $1 \leq i \leq q$, $1 \leq j \leq q+1$ である。

例3. Difference Set $(1, 2, 4, 10)$ は. Regular Array を構成する。

1	2	6	4
3	8	10	5
9	12	11	7

次にこの Regular Array の第1行から q 又はそれ以下の継続する元をとって Difference Triangle の第1行とする事により、Difference Triangle を構成する.

例4. 例3で元 (2, 6), (4, 1) は二つの三角

2 6　　4 1　　を構成する。

8　　5

この Difference Triangle の第1行を H マトリクスの第1列の1の元の間の間隔とする事により自己直交符号が得られる。

例5. 例4の三角について.

$[g_0^{(1)}, g_1^{(1)}, \cdots g_8^{(1)}]^T = 101000001$

$[g_0^{(2)}, g_1^{(2)}, \cdots, g_9^{(2)}]^T = 1001100000$

とすれば $R = 1/3$ 又は $2/3$ の符号が得られ、

$[g_0^{(3)}, g_1^{(3)}, \cdots g_{13}^{(3)}]^T = 1010000010001 1$

とすれば $R = 1/2$ の符号が得られる。

Robinson & Bernstein は 30 以下の素数のすべての巾に対する Regular array の組から Difference Triangle の第1行の元の和が最小となる符号を構成し、文献[5]に示している。第1行の元の和を最小とする事により、与えられた伝送速度 R, 距離 $d = J + 1$ に対して最短の拘束長を持つ符号が得られ、回帰符号の場合に重要である。

3. ブロック符号との比較

(i) Weldon [1] は Difference set cyclic code と

て Difference set を文の中として持つ多項式の Reciprocal Polynomial が H マトリクスを与える巡回符号を求めた。この符号は巡回性質を用いる事から正整数 S に対して $n = 2^{2S} + 2^S + 1$ なる符号長を持つ。これに対して回帰符号の符号長は、符号を定める Difference set の最大元で定められ、符号を定めるのに用いられた Difference set の modulus には無関係となる点も大きな相異である。然し同じ距離 $d = J+1$ を持つ符号は、同じ Difference set 又は同じ最大元を有する Difference set から構成されている。

表1

Weldon の符号と Robinson の符号（W, R で示す）

d		n 又は n_A	R	Difference set
4	W	7	3/7	0, 2, 3,
	R	8	4/8	同上
6	W	21	11/21	0, 2, 7, 8, 11
	R	24	12/24	0, 2, 7, 10, 11
10	W	73	45/73	0, 2, 10, 24, 25, 29, 36, 42, 45,
	R	92	46/92	0, 3, 9, 16, 20, 21, 35, 43, 45
18	W	273	191/273	0, 18, 24, 46, 50, 67, 103, 112
	R	402	201/402	115, 126, 128, 159, 166, 167, 186, 196, 201（両者共通）

(ii) Weldon の Self-Orthogonal Quasi Cyclic Codes [4] は Robinson & Bernstein の符号と殆んど同じようにして構成されるが、Quasi cyclic Property を得るために modulus m として Difference set が重複を持たず、且 disjoint である最小の整数 m を定める必要がある。この為同じ R, J を持つ符号でも其等の符号を生成する Difference set は相異なるものである場合が多い。

(iii) Goethals et. al. [3] は有限射影幾何学符号として、Balanced Incomplete Block Design (b, v, k, r, λ) を持つ符号を構成した。回帰符号の場合には、Massey によって $R = 1/b$ の符号の場合に示されている如く [6], L step orthogonal の符号は One step orthogonal となるから、Goethals et. al の符号を直接畳みこみ符号に拡張するわけにはいかない。然し、符号生成多項式

$$W(x) = x^{d_0} + x^{d_1} + \cdots + x^{d_s}$$

$$d_0 = 1 < d_1 < \cdots < d_s$$

を H マトリクスの第 1 列に取る事により、Rudolph [1] によって提案された「式」個の誤りを訂正する符号に対応する符号を求める事は出来る。このようにして構成される符号の能率は、然し乍ら、一般的によくない。

4、試行錯誤法による回帰符号の構成法

以上に論じて来た様に、回帰符号系のDesignにBalanced Incomplete Block Designを応用出来る範囲はごく限られている。現在迄にいくつかの有用な回帰符号系は試行錯誤法により導かれた。その数学的な導き方は未だ知られていない。ブロック符号系が種々の数学的性質を組込んで構成されて来たのに対し、多くの回帰符号系が試行錯誤法によって求められて来た事自身、回帰符号構成法の特徴の一つと考えられる。その二、三の例を以下に挙げる事とする。

(i)直交可能符号(Massey〔1〕)、直交可能符号は、パリティチェックマトリクスの行を加え合わせる事により$e_0^{(J)}$に直交するパリティチェックを得るものであり、一般に自己直交符号と同じR, Jに対して、拘束長を短かくする事が出来る。例えばR=1/2, J=6の自己直交符号は、$n_A=36$を持つのに対し、直交可能符号は$n_A=24$を持つ。これ等の直交可能符号は試行錯誤法によって構成され、その数学的構成法は1962年以来未解決の問題である。

(ii)バースト訂正回帰符号(岩垂〔8〕, Massey〔9〕)

バースト訂正回帰符号で任意の整数bにつきR=b-1/bを持つ符号は、閾値復号法による単一誤り訂正符号を交錯する事により得られるとも考えられる。そのシンドローム系列と

レて

$$S_I = E_b \underbrace{00\cdots0}_{r+b-2} E_{b-1} E_{b-1} E_{b-2} 0 E_{b-2} \cdots\cdots E_1 \underbrace{00\cdots0}_{b-2} E_1$$

$$S_{II} = E_b E_{b-1} 0 E_{b-2} 0 \cdots 0 E_1 \underbrace{00\cdots0}_{r+b-1} E_{b-1} E_{b-2} \cdots\cdots E_1$$

等が知られてソる。此等の符号も試行錯誤法によって求められた。組織的構成法は未だ知られてソなソ。

(iii) バースト及びランダム誤り訂正符号 (Massey [10], 岩垂 [11])。Massey は次の b-diffuse 符号を定義レた。

b-diffuse 符号: (イ) 直文数Jの自己直交符号または直交可能符号が復号される次1情報ビットから始まる長さb又はそれ以下のバーストは J/2 − 1 個以上のシンドロームビットに影響レなソ。(ロ) その他の場所から始まるバーストは高々J/2個のシンドロームビットに影響する。

この b-diffuse 符号は修正文錯法による R=1/2, J=4, 6 の符号を Massey [10] [12] が求め、普通の文錯法による符号が文献 [11] に求められてソる。現在迄のところ R=1/2, J=4, R=1/2, J=6 (Massey [10], [12], R=1/2, J=4, R=1/3, J=6, R=1/3, J=8 [11] の符号は単一バースト訂正符号としてガードスペースの下限を満す。一般に此等の符号は試行錯誤法によって求められ、数学的 Design に基づく組織的な構成法

は知られていない。

5. 結論

以上のように回帰符号のDesignはブロック符号のDesignより拘束が多く、いくつかの未解決の問題をかかえながら、符号の組織的構成法を求める事が難しい。組合せ数学の一層の応用により、回帰符号の組織的構成法を求める事は、回帰符号の今後の発展の重要な鍵となると考えられる。

文献

1. L.D. Rudolph, "a class of majority logic decodable codes," IEEE Trans. Information Theory, vol. IT-13, pp. 305-307 april 1967.
2. E.J. Weldon, Jr. "Difference-set cyclic codes," B.S.T.J. vol. 45, pp. 1045-1055, September 1966.
3. J.M. Goethals & P. Delsarte, "On a class of majority-logic decodable cyclic codes." IEEE Trans. Information Theory, vol. IT-14, pp. 182-188. March 1968.
4. R.L. Townsend & E.J. Weldon, Jr. "Self-orthogonal quasi-cyclic codes", IEEE Trans. Information Theory, vol. IT-13, pp. 183-195, April 1967.

5. J. P. Robinson & A. J. Bernstein, "a class of recurrent codes with limited error propagation," IEEE Trans. Information Theory, vol. IT-13, pp. 106-113, January 1967.

6. J. L. Massey, "Threshold decoding", M. I. T. Press, Cambridge Mass. 1963.

7. D. W. Hagelbarger, "Recurrent codes for the binary symmetric channel", lecture notes for the course Theory of Codes, University of Michigan Summer Conference, Ann Arbor, June 18-29, 1962.

8. 岩垂好裕 "バースト訂正回帰符号系の一理論" 電子通信学会論文誌 51-C pp. 549-556, 昭和43年12月.

9. J. L. Massey, Unpublished memorandum.

10. J. L. Massey, "Advances in threshold decoding" in "Advances in communication systems", A. V. Balakrishnan ed. Academic Press, New York 1968.

11. 岩垂好裕 "閾値復号法によるバーストおよびランダム誤り訂正符号系" 電子通信学会インホメーション理論研究会資料 IT68-40, 1968年11月

12. P. Voelcker, Private Communication, April 1969.